NCIX
NATIONAL COUNTERINTELLIGENCE EXECUTIVE

THE NRO/NATIONAL MILITARY INTELLIGENCE ASSOCIATION
COUNTERINTELLIGENCE SYMPOSIUM
Washington DC, 24 October 2007

Remarks by Joel F. Brenner
National Counterintelligence Executive

"Strategic Counterintelligence: Protecting America in the 21st Century"

Good morning, ladies and gentlemen. I'm glad to see so many of you at this symposium on counterintelligence issues facing our nation. And many thanks to our NRO hosts and to General Jim Williams and the National Military Intelligence Association for their gracious invitation to speak to you today.

Let me say right off the bat that addressing counterintelligence as a strategic capability is automatically challenging because we don't all have the same idea of what it is. This is true even on the DoD side. I'm going to sidestep that problem, however, by noting that dual-hatting Jim

Clapper across the civilian-military intelligence sectors was a brilliant stroke that should be the beginning – not the end, just the beginning – of far better military-civilian collaboration on counterintelligence. And I will address issues that confront all of us in this arena, whatever our definitional predilections.

The Strategic Issues

Three strategic challenges now confront the CI community: (1) threats to our cyber networks and opportunities to understand and counter them; (2) acquisition vulnerabilities created by the international nature of our markets; and (3) the need for better collaboration in countering espionage.

First, Cyber Networks: The nation's electronic networks are too easy to hack, and the number of world-class hackers is multiplying at bewildering speed. If you can exfiltrate massive amounts of information electronically from the comfort of your own office on another continent, why incur the expense and risk of running a spy or reconnaissance operation? If you can disrupt critical infrastructure electronically from the other side of the world, who needs a local saboteur? Our water and sewer systems, electricity grids, financial markets, payroll systems, and air- and ground-traffic control systems — to name only the most obvious — are electronically controlled and subject to sophisticated attack by both state-sponsored and free-lance hackers. These attacks can be designed to steal our nation's intellectual property or manipulate information to cause financial, logistical, or military chaos. You don't have to bring down a system to cause chaos. All you have to do is put bad information into it. If a system goes down, you know it's down. But if a military commander thinks he knows where he is on the face of the earth but really doesn't, or if a Wall Street trader think he knows the price of a security but really doesn't, the problem is even worse. The chaos may be slower in coming, but may also be more profound.

The poster child for this vulnerability is what happened in Estonia this past spring. Following a dispute with Russia over a World War II memorial in Tallinn, many of the computer systems in that former Soviet Bloc country were subjected to a massive denial-of-service attack resulting in significant governmental, economic, and social disruption. There have been large-scale denial-of-service attacks before, but this was the first such attack directed against a nation state as a whole, and it won’t be the last. We’ve got to do a better job of protecting our networks and thwarting adversary cyber intrusions.

The problem is strategic and a new frontier for counterintelligence. The Defense Department can’t fix it alone. The Intelligence Community, acting alone, can’t fix it either. Law enforcement still struggles with small-time hackers, never mind the kind of threat I’m talking about. To meet it, Director McConnell and the President are developing an integrated, national response. We need it, and I am confident we are going to get it.

The cyber challenge is beyond the old security paradigm — it’s not like making a better lock for a strong box full of secrets. The only way to eliminate entirely the risk of hacked or corrupted networks is to stop communicating and disconnect, and we’re not going to do that. Our systems are porous in part because they’re open. The problem, therefore, is more like managing the air flow through a large, segmented building in a polluted environment and filtering out the toxins in that air flow. At the end of the day, we have to deliver fresh air safe for breathing.

We’ve really got three related but different problems here: hardware vulnerabilities, software vulnerabilities, and human behavior. Of the three, human behavior is by far the most difficult to manage. I know of a case in which some guy (a contractor, by the way) nearly brought down an entire agency’s unclassified systems when he decided he was too smart to use the equipment issued to him and hooked up his own device to the agency’s network. And what do you know? It was infected.

This week I learned of another smart guy who, after taking his PDA to a foreign country well known for cyber intrusions, synched it up to his agency’s networks. The risk that he has infected his agency’s servers with a “phone home” vulnerability approaches 100%. But gosh, not being able to synch your personal calendar and contacts with your office systems is a real pain in the neck ….

When convenience butts heads with security, convenience wins – hands down, every time. And when you add stupidity, malice, and carelessness to the mix – and I’m afraid we find those qualities in some measure in every organization, public or private -- you have the makings of serious cyber management problems.

If you want to make your self less vulnerable to identity theft, you need to choose strong passwords, keep them secret, and change them periodically. You also need to encrypt what’s on your computer, apply software patches as soon as they become available, install strong firewalls, and so forth. How many of you do that?

Businesses and governments have to do these same things — only more of them and at industrial strength – and our record, and their record, are mixed at best, to put it mildly. We don’t manage our systems and the people who use them as well as we could, and we don’t do it consistently. We need to change that. This includes monitoring bad behavior on our systems.

When I say “our” systems, I include private firms and universities. We in government can do a better job of helping you handle cyber vulnerabilities through a better warning system. Specifically, our rules for what we can tell you (our “cooperation model,” if I may put it that way) is a function of our classification model. That is, if you're doing classified work, we can and may provide you with information about actual or potential attacks on your system that we cannot provide if you're not working on a classified contract. The problem with this cooperation model is that it assumes that the criticality of your systems depends on whether you're doing classified work – which generally means defense-intelligence work. This assumption is antiquated. The Critical Infrastructures Protection Act of 2001 defines "critical infrastructure" to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[1] And the Homeland Security Act of 2002 defines "key resource" to mean "publicly or privately controlled resources essential to the minimal operations of the economy and government."[2] These definitions have nothing to do with the system for classifying information – nor should they. So we've got work to do here.

[1] 42 USC § 5195c(e).

[2] 6 USC § 101(10).

Acquisition: Now let me tell you what I meant when I mentioned “acquisition risk” as a strategic CI issue. Businesses and government, including intelligence agencies, buy communications and other equipment in the open international market. What are we buying? What does “Made in USA” mean when components come form overseas and the software in the electronics may have been written by God-only-knows-whom? Unknown or sketchy provenance raises the risk that a foreign government or organization could program vulnerabilities into our most sensitive information systems.

We are now putting more resources against this problem, and we are getting much more rigorous in our analytic approach to it. It may be appropriate that different agencies or businesses have different tolerances for acquisition risk, but it is not appropriate that, under the guise of managing risk, we kid ourselves about what the risk really is. Risk management is not risk acceptance. Which is why we must employ a consistent risk assessment methodology across the intelligence community and, eventually across the entire federal government.

Doing rigorous and consistent analysis is only part of the problem, however. When you confront an agency at the end of its procurement process with an objection to what it proposes to do, you're immediately pegged as an impediment to mission. So the challenge is to integrate our evaluations early in the acquisition process so we can be a constructive and non-confrontational player in acquisitions before positions become set in concrete. This is easier said than done, but with high-level direction, we can do it.

Collaboration: Now let me address the old-fashioned problem of collaboration — by which I mean getting different parts of the government playing like they're really on the same team. When Congress passed the statute that created my position in 2002, one of their objectives was to improve the coordination of counterintelligence activities to make them more efficient and effective.

Step one in addressing collaboration was to rejuvenate the National CI Policy Board, which I did. It had not met in at least 18 months. The Board now meets monthly and accomplishes real work, much of it through a series of working groups. The Board's priority over the past year was the development of the National CI Strategy, which the President has approved and which you can see in unclassified version on our website. Our priority now is to push that Strategy from the clouds down to the sidewalk.

When you think about collaboration, think about a continuum of joint activity. At the weakest end of that continuum is deconfliction. We're pretty good at that, especially in operations, sometimes in policy: *You stay out of my way, and I'll stay out of your way.* But that's a pretty low bar and nothing to brag about. Somewhere in the middle of this continuum is cooperation: *I can't manage this problem or this target alone; can you help?* Here I think our record is spotty, though in some critical areas, such as the mostly excellent bilateral relationship between the FBI and CIA, we're much better than the public realizes, particularly at the tactical level; and overall we are in much better shape than we were in 2001. At the strongest end of the continuum is collaboration. This is joint work and shared responsibility, and it has to start at the planning and budgeting stage. *Here's the problem: How do we attack it together?* As a general rule, we're not there yet.

Sometimes I'm challenged when I urge collaboration with the objection that I'm ignoring "lanes in the road." Let me tell you something: *A lane in the road is a horizontal stovepipe.* Take a stovepipe, rotate it 90 degrees, and you've got a lane in the road. Having said that, however, when we collaborate successfully, we have obviously got to pay attention to the competencies and legal authorities of the agencies that are working together on the same and related targets. But make no mistake about it: Collaboration is what the country expects from us, and we will rise or fall as an intelligence community on our willingness and ability to do it.

Changing the expensive and cumbersome system we are using to bring people into sensitive government activities illustrates this point about collaboration. Our colleagues in the security discipline are confronting big changes in the way we clear and monitor a trusted workforce. For a long time we have spent too much money, and too much time, on vetting people at the threshold – and spending it inefficiently, I might add. Meanwhile, we spend next to no time and money in vetting people's activities after they get cleared. Under Director McConnell's insistent leadership, this is changing. We are now putting in place an interagency process to test security clearance reforms and establish risk management parameters we can live with. Are we getting it right? I don't know yet. Will we increase counterintelligence risk as we bring in native speakers and higher-risk operators? Without a doubt. Am I concerned about that? Sure. And we are going to have to manage that risk, watch the new processes like a hawk, and certainly recalibrate them from time to time.

The single most important factor in developing a more collaborative culture in the intelligence community is Director McConnell's joint duty initiative. Soon it will no longer be possible to achieve senior status in the intelligence community without having had substantial experience in more than one agency. We are creating by regulation what the Congress created by statute for the military in 1986 by the Goldwater-Nichols Act, which transformed the organization and culture of our military so that today the military is far ahead of the civilian side of government in its ability to collaborate across organizational boundaries. With the joint duty initiative, however, the intelligence community is going to catch up.

Global Trends

There are two trends underway in the business world that will affect the way intelligence practitioners work in the future. They are not specific to counterintelligence, but they are bound to affect us along with the rest of the community. One relates to the "unbundling" of activities that were bundled or aggregated earlier in our history. The other involves the "disintermediation" of activities, how goods and services are more directly delivered today than in times past. These are two big waves that the intelligence community has mostly ducked – *so far*.

"Unbundling" means separating once-aggregated activities into separately priced components. Think back to the way telephone service was delivered before the late 1970s when the Bell System was broken up. There was one phone company, and that company sold you equipment, wiring and installation services, local phone service, and long distance service too. When that cozy world fell apart, it was a big nuisance for consumers. People had to make choices and didn't always like it. "Telephone service," conceived as a unitary product, got unbundled, and suddenly we bought different pieces of it from different firms. The benefits of the resulting competition have been dramatic, and without that competition, we would not have had the telecommunications explosion of the last few decades – or rather, the US would not have led that explosion.

We could multiply examples: hospital care, banking, energy generation and transmission, and so on. Unbundling pushes competition (and therefore efficiency) deeper into the economy. It would not surprise me if some of the several distinct parts of the business of intelligence got unbundled too, particularly on the analytic side. In fact, it would surprise me if this did not happen.

"Disintermediation" means taking the middle man out of the market. You want shoes? You don't have to visit the shoe store any more. You can buy them online. The same goes for clothes, financial securities, books, automobiles, and lots of other products. Electronic transactions are displacing specialized brokers in the financial services industry. In news delivery, there is a proliferation of sources of unfiltered information, blurring the very definition of journalist. You want information? Who needs a newspaper anymore? (I think I do, but plummeting circulations tell us that lots of people don’t. And as for me, I don’t need the *whole* newspaper; I can pick and choose pieces from this one or that one, and I do.)

This trend is bound to affect intelligence – again, particularly on the analytic side.

Who’s the middle man in the delivery of intelligence to policy makers? Analysts. What’s the difference between an analyst and a journalist or editor? Why should we think that the market and social forces that are transforming journalism will leave intelligence analysis alone? They won’t. The role of “finished” intelligence has begun to diminish as analytic and other intelligence activities are disaggregated and provided more directly to consumers. Look at the internet and you can see the world moving toward raw intelligence and away from established or finished intelligence products.

The world is also moving toward *private* intelligence. The corporate world creates, commissions, and buying intelligence analysis to a degree that would surprise many of our colleagues. And one reason they can do it is that governments no longer have a monopoly on world-class collection vehicles, like satellites, and world-class communications equipment. On a long historical view, beyond the last century, private intelligence is not new. In 1815, the best intelligence on the results of the Battle of Waterloo belonged to the Rothschilds – a system of beacons from Belgium, across the Channel, up to London. That's how they learned of Napoleon's defeat before anybody else, including the government, and made a fortune on Consols (the British equivalents of Treasuries).

The pressure on collection will be slightly different. If you're on a watch floor and you learn from a secret source about a sudden event in, say, Kabul, and then 25 minutes later a report of that event appears on CNN, how many tens of millions are you willing to pay for that secret source? A rational answer should depend on two factors: (1) The dependability of open sources, and (2) whether you can do something significant with the information in the 25 minutes before everyone else knows about it (as Rothschild did). To an increasing degree, I suspect we are going to be unwilling to make that investment. But whether we do or not, I predict that in the future, the critical factor in more and more (though not all!) situations will be speed rather than secrecy.

This will sound strange to those of us who spend most of their time dealing with truly, deeply secret material. So please don't misunderstand me. There is always going to be secret material. What I'm saying is that less and less will be secret and that much of it won't stay secret for very long, and speed of moving information and acting on it will therefore be at a premium.

Unbundling and disintermediation are happening whether we like it or not, and these forces will shape the future. Our purpose will still remain: To describe the world as we think it is and to forecast what it probably will be. But as Director McConnell wisely tells us, we're going to have to change some of the ways we do business. In closing, let me say this: In the intelligence community we are blessed with formidable intellects, formidable experience, and formidable tools. At this juncture, when our world is in flux, our greatest challenge may be to turn these tools on ourselves.

###